Securing IoT Devices with Manufacturer Usage Descriptions

Eliot Lear

Principal Engineer, Enterprise Chief Technology Office

10 Apr 2019

Today’s latest threat: printers

Study cites multi-function printers as some of the most dangerous members of the IoT family

Bitdefender.com, 28 February 2019

What Sort of Access Do These Printers Require?

From	To	Protocol	Source Port	Destination Port(s)
Printer	xmpp009.hpeprint.com	TCP		80, 443, 5222,5223
Printer	DNS Server	UDP		53
Printer	chat.hpeprint.com	TCP		80,443
Printer	224.0.0.251/32	UDP		5353
Printer	220.0.0.252/32	UDP		5355
Printer	h10141.www1.hp.com	TCP		80
Printer	Local Networks	UDP	5353	
Printer	Local Networks	TCP	80	

Source: University of New South Wales, using mudgee

(not shown: L2 packets)

Our First Three Questions

- Is that information correct?
  - Maybe: Not sourced from vendor
- How does the administrator learn it?
  - Scanned network for some number of days
- What vulnerabilities does that device have?
  - Can’t tell because we probably don’t have model information

And consider how much time it will take for that one device.

Assumptions and Assertions

Assumptions	Assertions
A Thing has a single use or a small number of uses.	Because a Thing has a single or a small number of intended uses, all other uses must be unintended.
Things are tightly constrained. Very little CPU, memory, and battery.	Any intended use can be clearly identified.
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to provide guidance to administrators.
Even those Things that can protect themselves today may not be able to do so tomorrow	A mechanism is needed to protect devices that may have vulnerabilities.

Translating intent into config

Any intended use can be clearly identified by the manufacturer

```
access-list 10 permit host
controller.mfg.example.com
```

All other uses can be warned against in a statement by the manufacturer

```
access-list 10 deny any any
```

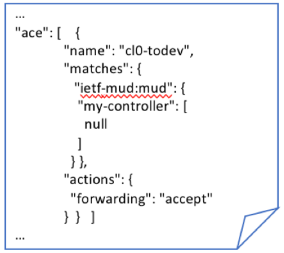
Introducing Manufacturer Usage Descriptions (MUD)

A URL:

https://manufacturer.example.com/mydevice.json

The MUD Manager:

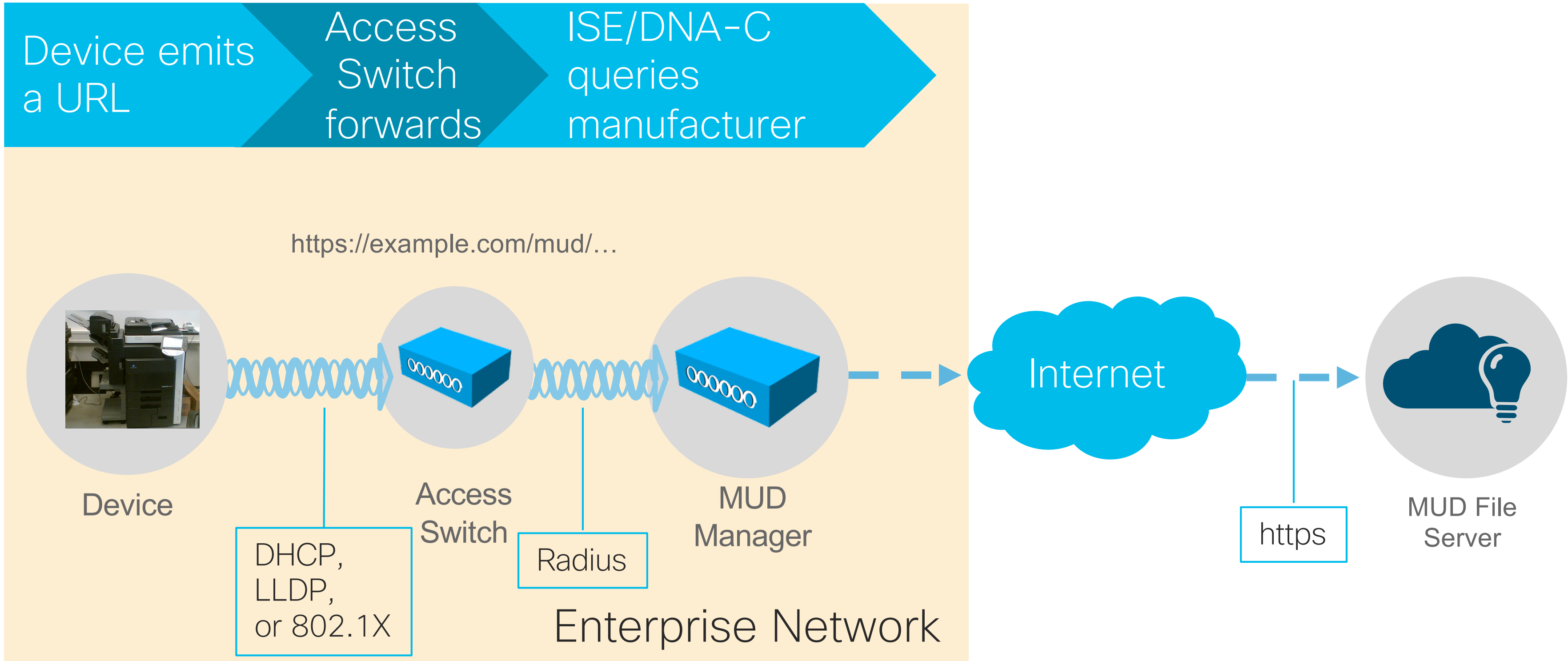
A MUD File:



```
...
"ace": [    {
          "name": "cl0-todev",
          "matches": {
            "ietf-mud:mud": {
             "my-controller": [
              null
             ]
           } },
          "actions": {
           "forwarding": "accept"
          } }  ]
...
```

The MUD File Server:

Expressing Manufacturer Usage Descriptions



Device emits a URL

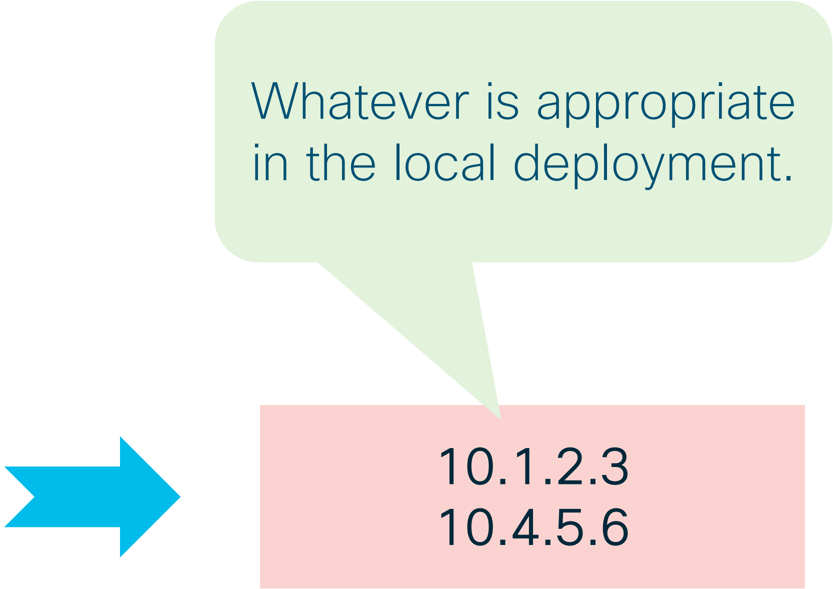
Access Switch forwards

ISE/DNA-C queries manufacturer

https://example.com/mud/…

Getting from the MUD file to deployment config

```
... "acl": [
      {
        "name": "mud-76228-v4to",
        "type": "ipv4-acl-type",
        "aces": {
          "ace": [
            {
              "name": "myctl0-todev",
              "matches": {
                "ietf-mud:mud": {
                  "my-controller": [
                    null
                  ]
                }
              },
              "actions": {
                "forwarding": "accept"
              } ...
```



Whatever is appropriate in the local deployment.

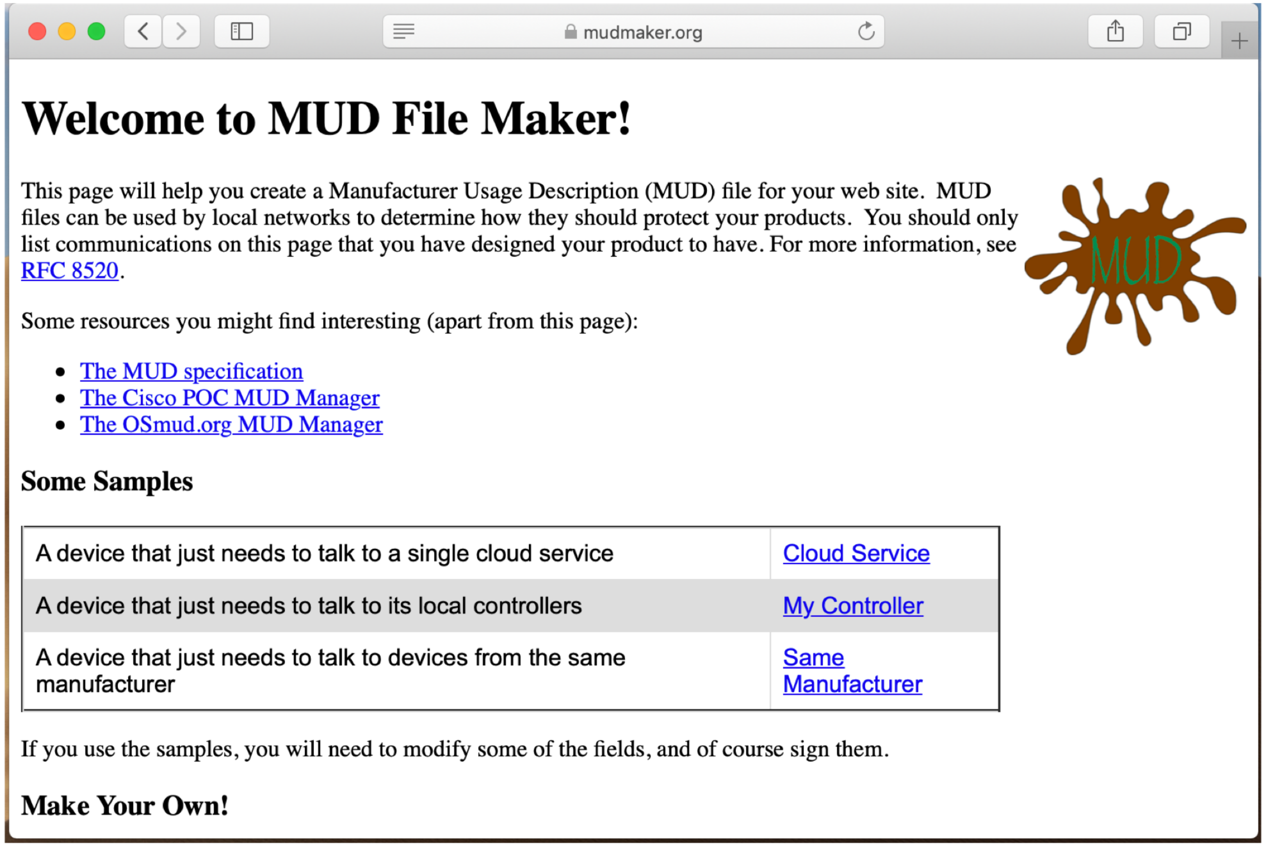
10.1.2.3
10.4.5.6

https://mudmaker.org

Manufacturers Use Classes

Class	Used for	Filled in by
Domain name	Cloud-based controllers	IOS
(My) Controller	Access to controllers	Administrator
same-manufacturer	Access to devices that are built by the same manufacturer	MUD Manager
Manufacturer	Access to devices that are built by specified manufacturer	Manufacturer and MUD Manager
Local	Used when device needs access to the local network	Administrator

Make Your Own MUD File



Welcome to MUD File Maker!

This page will help you create a Manufacturer Usage Description (MUD) file for your web site. MUD files can be used by local networks to determine how they should protect your products. You should only list communications on this page that you have designed your product to have. For more information, see RFC 8520.

Some resources you might find interesting (apart from this page):

- The MUD specification
- The Cisco POC MUD Manager
- The OSmud.org MUD Manager

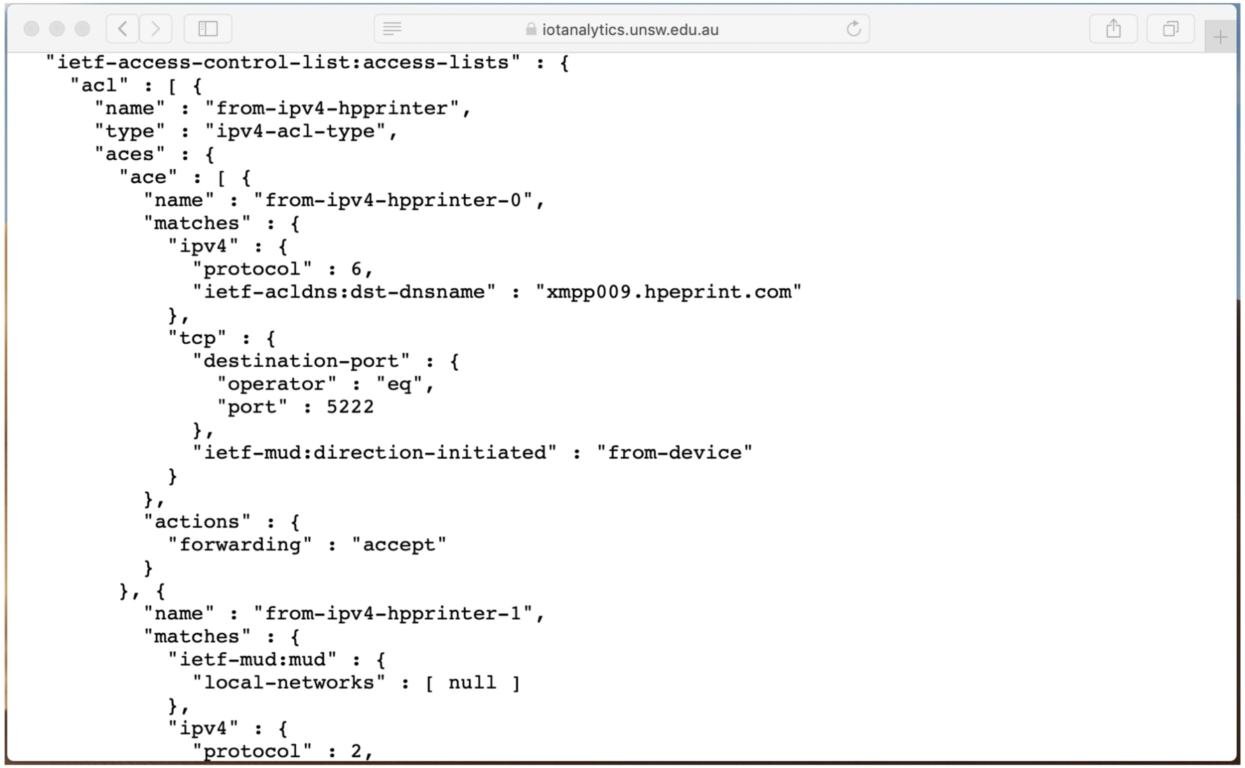
Some Samples

A device that just needs to talk to a single cloud service	Cloud Service
A device that just needs to talk to its local controllers	My Controller
A device that just needs to talk to devices from the same manufacturer	Same Manufacturer

If you use the samples, you will need to modify some of the fields, and of course sign them.

Make Your Own!

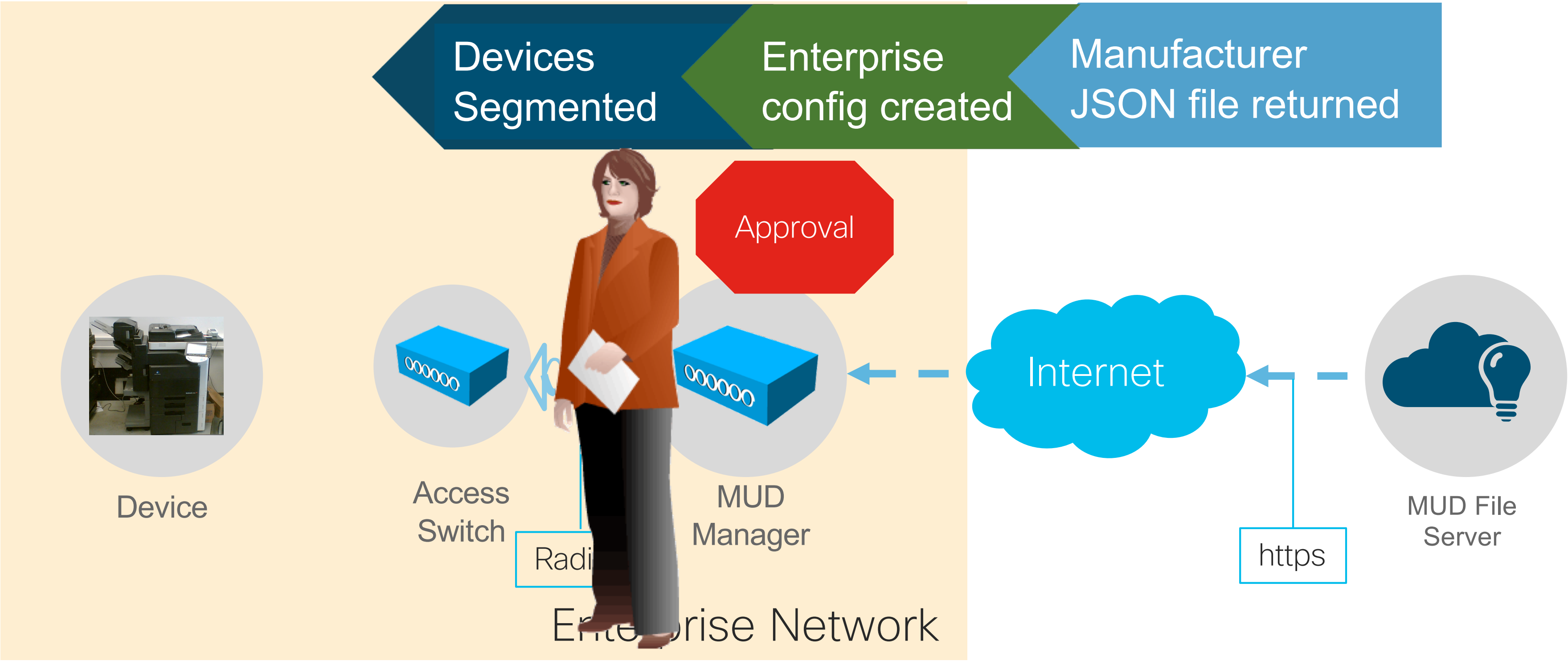
So for instance…



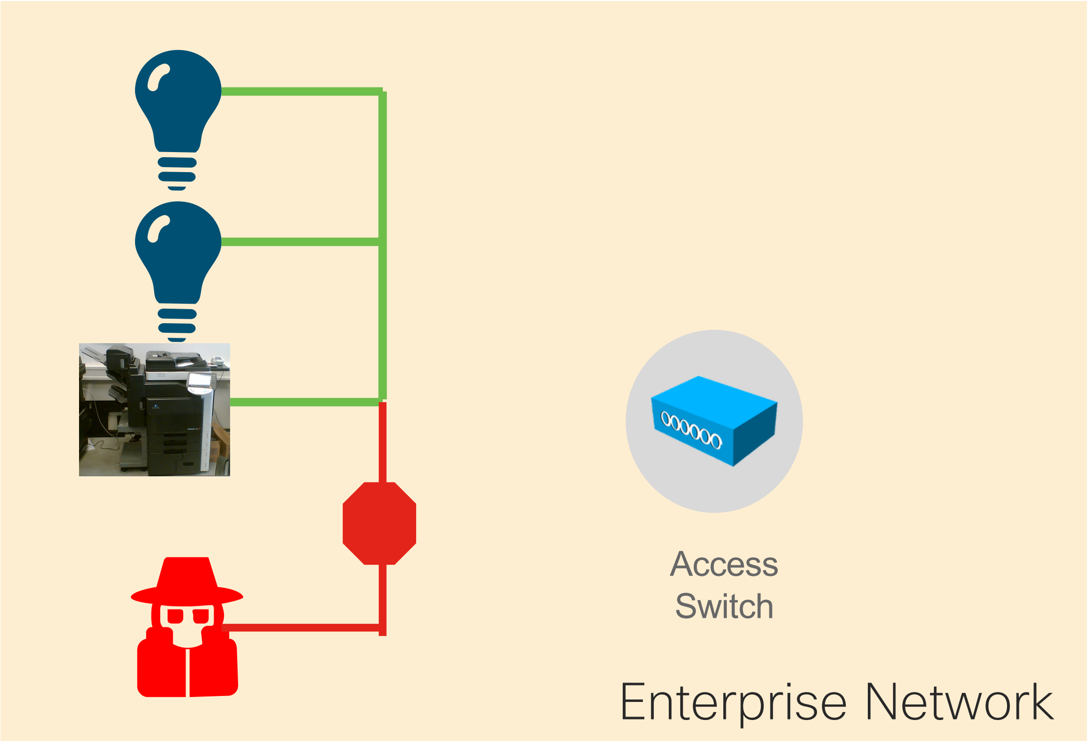
```
  "ietf-access-control-list:access-lists" : {
    "acl" : [ {
      "name" : "from-ipv4-hpprinter",
      "type" : "ipv4-acl-type",
      "aces" : {
        "ace" : [ {
          "name" : "from-ipv4-hpprinter-0",
          "matches" : {
            "ipv4" : {
              "protocol" : 6,
              "ietf-acldns:dst-dnsname" : "xmpp009.hpeprint.com"
            },
            "tcp" : {
              "destination-port" : {
                "operator" : "eq",
                "port" : 5222
              },
              "ietf-mud:direction-initiated" : "from-device"
            }
          },
          "actions" : {
            "forwarding" : "accept"
          }
        }, {
          "name" : "from-ipv4-hpprinter-1",
          "matches" : {
            "ietf-mud:mud" : {
              "local-networks" : [ null ]
            },
            "ipv4" : {
              "protocol" : 2,
```

(Just a snippit)

Expressing Manufacturer Usage Descriptions



Results: Micro-segmentation of that printer



- Access limited to devices based on manufacturer recommendations
- Policy choices easily identified by MUD file
- Hacked devices can’t probe for holes
- An additional layer of security
  - BUT- manufacturers should still **always** secure their devices

Next Steps

- More MUD tooling
- MUD for 5G
- More implementations!

Thank You!

Credit to… (Creative Commons Licensing)

- The Printer https://en.wikipedia.org/w/index.php?curid=16404543